电脑使用导航（2）

电脑病毒防范与硬盘故障修复

希武图书软件工作室　钟希武 尹春燕　编　写

北京希望电子出版社
Beijing Hope Electronic Press
www.bhp.com.cn

电脑使用导航（2）

电脑病毒防范与硬盘故障修复

希武图书软件工作室　钟希武 尹春燕　编　写

北京希望电子出版社
Beijing Hope Electronic Press
www.bhp.com.cn

内 容 简 介

本书专为电脑新手编写。作者对电脑用户常遇到的电脑病毒、普遍要使用的杀毒软件及其使用方法、硬盘故障与修复进行了介绍，使电脑新手基本可以应付电脑使用过程中遇到的病毒与硬盘故障问题。

本书共由 8 章组成。主要包括电脑病毒的危害、病毒黑名单部分介绍了 28 种常见病毒、国内杀毒网站大阅兵，讲述了 5 个网站、国外杀毒网站大阅兵，介绍了 3 个网站、国内有代表性杀毒软件评述，列举了 4 种软件、国外有代表性杀毒软件评述了 2 种软件、防火墙部分介绍了 6 种功能较强的防火墙、硬盘故障与修复。

本书的特点：内容丰富、指导性强、即学即用。本书可以作为初中级电脑用户的实用指导书。

本版 CD 内容为电子书。

系 列 盘 书 名 ：电脑使用导航（2）
盘　　书　　名 ：电脑病毒防范与硬盘故障修复
文 本 著 作 者 ：希武图书软件工作室　钟希武 尹春燕
责 任 编 辑 ：周艳
C D 制 作 者 ：希望多媒体开发中心
C D 测 试 者 ：希望多媒体测试部
出版、发行者 ：北京希望电子出版社
地　　址 ：北京市海淀区知春路甲 63 号卫星大厦三层 100080
网址: www.bhp.com.cn，E-mail:zwb@bhp.com.cn
电话: 010-62520290,62521724,62528991,62630301,62524940,62521921,
82610344（发行） 010-82675588-202（门市） 010-82675588-501,82675588
-201（编辑部）
经　　销 ：各地新华书店、软件连锁店

排　　版 ：希望图书输出中心　全卫
C D 生 产 者 ：北京中新联光盘有限责任公司
文 本 印 刷 者 ：北京广益印刷有限公司
开本 / 规格 ：787 毫米×1092 毫米　16 开本　15.5　印张　22 千字
版次 / 印次 ：2003 年 3 月第 1 版　2003 年 3 月第 1 次印刷
印　　数 ：0001-5000 册
本　版　号 ：ISBN 7-89498-105-2
定　　价 ：22.00 元（本版 CD）

作 者 简 历

钟希武 原为天津某大型商业公司电脑部主任，开发有多项应用系统。在国家级刊物上发表过多篇论文。曾兼任《香港电子》、《多媒体用家》、《PC 用家》特约编辑及专栏撰稿。从 1998 年起建立天津希武图书软件工作室。现为职业撰稿人，高级工程师。

从 1993 年起，先后在台湾《印刷科技》、《倚天》、《资讯与电脑》、《大家用电脑》、《第三波》、《PC DIY!》、《XMAGAZINE 杂志》、《新电子》及香港《今日电脑》、《现代电脑》、《无线电技术》、《多媒体专刊》、《国际通讯》、《微型电脑专刊》、《香港电子》、《多媒体用家》、《PC 用家》等媒体及国内的《微型计算机》、《电脑报》、《中国计算机报》等二十多家刊物上发表过二百多篇技术文章（300 余万字），同时还发表了 30 多篇综述与新闻报道。著有《电脑硬体鉴别经验谈 531 问》（台湾旗标出版公司 97 年出版）、《多媒体电脑选购 875 问》、《99 DIY 电脑硬件选购经验谈》、《DIY 2000 电脑硬件选购指南》、《DIY 2002 最新电脑硬件技术大全》等多本书，共计 350 多万字。

最大业余爱好有两个：其一是收藏、研究“文革”时期的毛泽东像章及珍贵文史资料。并为其中最有代表性的 千枚像章配有 15 万字文字说明。其二是编写爱情小说及电视剧本，有 20 集电视剧本《纯真爱情》即将出版。希望就毛泽东像章在光盘开发、图书出版、展览以及电视剧本等方面进行合作。

尹春燕 现为南开大学教育部重点实验室高级工程师，曾多次在国家级刊物上发表多篇论文。有科研成果荣获国家省部级科技进步一等奖。先后在香港《现代电脑》、《多媒体专刊》、《国际通讯》、《微型电脑专刊》、《多媒体用家》、《PC 用家》等媒体及国内的十余家刊物上发表数十篇文章。与钟希武合作出版过六本书。

目　录

第 1 章　电脑病毒的危害 1
1.1　电脑病毒的定义 1
1.2　电脑病毒的命名 1
1.3　电脑病毒的类型与特点 2
1.4　防御电脑病毒 3
1.5　杀毒软件的使用技巧 5
1.6　病毒识别、防范技巧 6
1.6.1　宏病毒的识别技巧 6
1.6.2　宏病毒的防范技巧 6
1.6.3　邮件病毒的防范技巧 7
1.6.4　特洛伊木马病毒的识别技巧 7
1.6.5　特洛伊木马病毒的防范技巧 8
1.6.6　恢复系统技巧 8
1.6.7　防止病毒发作的技巧 9
第 2 章　病毒“黑名单” 10
2.1　全球前 7 名网络病毒 10
2.1.1　W32.Liac.A@mm 10
2.1.2　W32.Fishlet.A@mm 10
2.1.3　Klez 11
2.1.4　Nimda 11
2.1.5　Worm.Sircam 12
2.1.6　ILOVEYOU 13
2.1.7　HappyTime 13
2.2　全球前 10 名宏病毒 14
2.2.1　MakeLove 14
2.2.2　WordPro.Spenty 14
2.2.3　X97M.Ellar.E 14
2.2.4　X97M.Draco 15

2.2.5 W97M/Shore.p.....15
2.2.6 W97M.Comical@mm.....15
2.2.7 W97M.Cerin.A.....16
2.2.8 WM/Theatre.A.....16
2.2.9 WM97/Blowup-A.....16
2.2.10 W97M.Camino.A@mm.....16
2.3 全球前 10 名特洛依木马病毒.....17
2.3.1 TROJ_KALM.A.SVR.....17
2.3.2 红色代码 II.....17
2.3.3 Trojan.Nethief10.....18
2.3.4 Liquid.....18
2.3.5 GirlGhost2.....18
2.3.6 W32.Whiter.Trojan.....18
2.3.7 Trojan.MircAbuser.....19
2.3.8 TROJ_MANDRAGORE.....19
2.3.9 TROJ_PARODY.....20
2.3.10 PE_MAGISTR.A.....20
2.4 Windows 病毒.....21
CIH.....21
第 3 章 国内杀毒网站大阅兵.....22
3.1 瑞星网站.....23
3.2 金山毒霸网站.....29
3.3 江民网站.....37
3.4 北信源网站.....41
3.5 东方卫士网站.....47
第 4 章 国外杀毒网站大阅兵.....54
4.1 symantec（赛门铁克）.....54
4.2 McAfee 杀毒之星.....63
4.3 Panda Antivirus（熊猫卫士）.....72
第 5 章 国内有代表性杀毒软件评述.....78
5.1 瑞星杀毒软件.....78

5.1.1 软件介绍 78
5.1.2 软件特点 78
5.1.3 软件安装 79
5.1.4 使用说明 81
5.2 金山毒霸 2002 92
5.2.1 软件介绍 93
5.2.2 软件特点 93
5.2.3 软件安装 94
5.2.4 使用说明 94
5.2.5 金山网镖 2002 102
5.3 KV3000 杀毒王 105
5.3.1 软件介绍 106
5.3.2 软件特点 106
5.3.3 软件安装 108
5.3.4 使用说明 110
5.4 熊猫卫士钛金版 115
5.4.1 软件介绍 115
5.4.2 软件特点 116
5.4.3 软件安装 117
5.4.4 使用说明 121
第 6 章 国外代表性杀毒软件评述 132
6.1 Norton AntiVirus 2002 132
6.1.1 软件的安装 132
6.1.2 使用说明 137
6.1.3 病毒防火墙 142
6.1.4 邮件监测 143
6.1.5 病毒扫描设置 143
6.1.6 总结 145
6.2 Virus Buster2002 145
6.2.1 软件安装 145
6.2.2 使用说明 146

第 7 章　防火墙 163
7.1　天网防火墙 163
7.1.1　软件特点 163
7.1.2　软件安装 164
7.1.3　使用说明 167
7.2　蓝盾防火墙 172
7.2.1　软件特点 173
7.2.2　软件安装 173
7.2.3　使用说明 174
7.3　瑞星个人防火墙 179
7.3.1　软件特点 179
7.3.2　软件安装 181
7.3.3　使用说明 182
7.4　反黑王 187
7.4.1　软件特点 187
7.4.2　软件安装 188
7.4.3　使用说明 190
7.5　诺顿个人防火墙 194
7.5.1　软件特点 195
7.5.2　软件安装 195
7.6　网络保护神 211
7.6.1　软件安装 212
7.6.2　使用说明 218
7.7　防火墙技术问答 220
第 8 章　硬盘故障与修复 223
8.1　新型硬盘的防护技术 223
8.2　使用技巧及“软”故障排除 224

第 1 章　电脑病毒的危害

从广义上定义，凡能够引起电脑故障，破坏电脑数据的程序统称为电脑病毒。

电脑病毒是客观存在的一种具有破坏性质的程序，我们不能否认它的存在，更不能忽视它对电脑和电脑系统所造成的危害。其危害表现为：破坏硬盘分区表；破坏、重写硬盘 DOS 系统或 BOOT 引导区；破坏程序文件、数据文件；影响系统运行速度；格式化、删除部分文件内容；使被感染、覆盖的程序或文件的长度增大。经常使用电脑的用户都会对电脑病毒有谈虎色变的感觉，因为，电脑病毒是一种可以肆无忌惮的进行破坏和传染的可怕程序。当电脑病毒发作时，一般都会出现不能正常启动电脑，某些程序不能正常运行、莫名其妙地死机、突然重新启动电脑，程序运行速度极慢、程序图标改变、突然出现黑屏、蓝屏、屏幕出现特定的程序画面，比如女鬼病毒等。

1.1　电脑病毒的定义

电脑病毒（Computer Virus）是一个程序，一段可执行代码，它是具有破坏电脑数据、引发电脑故障的程序。通常，电脑病毒是具有强大而又独特的复制能力（对病毒载体），它可以以难以想象的速度迅速蔓延，同时又很难对它进行清除和防范。再有，电脑病毒都应具有一定的共性，主要表现在有破坏性、隐蔽性、潜伏性、传染性等几个特征。比如，通过磁盘、网络等媒介传播感染其它程序，复制并借助载体，使其具有一定的潜伏性、隐蔽性。当电脑系统符合某种特定的条件或时间时，

病毒体会自动进行复制、传播、破坏数据等。我国于 1994 年 2 月 18 日正式颁布了《中华人民共和国计算机信息系统安全保护条例》，在第二十八条指出“电脑病毒，是指编制或者在电脑程序中插入的破坏电脑功能或者毁坏数据，影响电脑使用，并能自我复制的一组电脑指令或者程序代码。”，从而在不同的意义上给电脑病毒制定了一个具有法律性、权威性的定义。

1.2　电脑病毒的命名

电脑病毒的种类数不胜数，而一种电脑病毒往往又会有很多名字，比如 Hybris 病毒（白雪公主病毒）有些网站称其为 W32/Hybris.gen.dll@M、W32/Hybris.plugin@M、

W32/Hybris.gen@M、TROJ_HYBRIS.A、I-Worm.Hybris 等，目前给病毒命名工作在国际上也无法得到协调，这就造成了人们在讨论病毒时，谈论了很多不同名称的病毒，

其实都是一种病毒，只是在名称上有所不同罢了。国内、国际反病毒软件厂商对于病毒的命名也是不尽相同，但大都是殊途同归，在病毒的命名上是取决于病毒发作时间、病毒发作症状、病毒表现形式、病毒自身标志、病毒工作机理、病毒发源地、病毒发现者、病毒代码长度等几种方法。之所以为电脑病毒命名，其目的就是使电脑用户更快速、准确的识别、防范和清除电脑病毒，因为电脑病毒被命名后可以以更客观的方法体现出该病毒的特征，使该病毒不容易与其它电脑病毒混淆。

对于目前多如牛毛的电脑病毒，本来就使电脑用户不寒而栗，头痛不已，然而，一些恶作剧者、蓄意破坏者、存有报复心理的程序员，以及为了经济利益、政治目的、军事目的的病毒制造者，时时刻刻都在编造着各种各样的电脑病毒。同时，我们的反病毒厂商都在一丝不苟的注视着电脑病毒的变化，客观的说，有了他们这种兢兢业业的精神，破坏程度再大的电脑病毒，我们也不用害怕。当然，这种说法是不绝对的，有些病毒为了逃避、抵抗反病毒软件的八面堵截，以及为了增强病毒的破坏力、兼容性，病毒制造者在不断完善病毒自身的抵抗能力，从而使病毒轻易逃避反病毒软件的追杀，这样的病毒，我们称其为该病毒的变种。

一般情况，变种病毒是通过对原病毒的内部模块、表面模块、传染模块、破坏模块等进行反编辑、修改，使其成为一种基于原病毒体而又不同于原病毒体的新生病毒体。变种病毒又可简单的分为两种变种，一种是简单对原病毒体的显示信息等内容加以改动，而对传染模块等关键代码不做改动，另外一种是修改原病毒体的重要代码，修改后，此病毒将以全新的机制工作。再经过不断的演变，就会演化为一种新的病毒，这一点与生物界内的病毒演化方式是相同的。为了准确捕捉、防范、清除新病毒，反病毒界的专业人员就必须不断分析病毒的传染机制、病毒体代码等重要模块，否则，将无法对付越来越多的电脑病毒。

1.3　电脑病毒的类型与特点

从第一个电脑病毒出世以来，究竟世界上有多少种病毒，客观的解释，应该没有确切的数字，虽然在各界有着不同的说法，但这个量化的数字实在是没有人能回答出来。无论多少种病毒，这只能代表着它的历史数据，因为在每时每刻，病毒的数量始终在不断增加。据国外专业机构统计，电脑病毒正以 15 种/周的速度不断递增。但无论再多的病毒如何快速繁殖，其种类也不超过我们所了解的几种类型，为了让不同的电脑用户更好的了

解病毒，电脑病毒可以按照攻击的系统分类、破坏程度分类、传染性分类、寄生方式分类、传播途径分类等，对于这么多的分类方法，恐怕电脑用户会对电脑病毒更加困惑和恐惧，再加上病毒的类型可以从很多种特定的含义进行分类，可我们不需要从这么多方面了解病毒的病理，因此，我们以最常用的分类方法。按照传染性将电脑病毒简单分类，可以分为磁盘引导区病毒、操作系统病毒、可执行程序病毒三种病毒。但由于电脑病毒的数量不断剧增，单凭三种类型很难将每种病毒归类，因此，可以将病毒的类型细分为引导型病毒、DOS 病毒、Windows 病毒、文件型病毒、网络病毒、蠕虫病毒、宏病毒等，再有，特洛伊木马（Trojan horse）和逻辑炸弹（Logic bombs）也应归属于病毒家族里的一员，尤其是逻辑炸弹，它虽然没有传染性，但具有象病毒一样的破坏性、隐蔽性和潜伏性，通常这种程序只有当特定事件出现时才会对硬盘数据进行恶意破坏，所以它也应算是病毒的一种。

1.4　防御电脑病毒

保持电脑系统干净是每一位电脑用户梦寐以求的事情，然而，电脑病毒的存在却不能保证电脑系统的清洁，当然，用户可以使用杀毒软件等产品来保护电脑系统，但杀毒软件是不能起到绝对性的作用，因为杀毒软件是针对已经出现的电脑病毒，这样可能会被刚出现的新病毒钻了空子，更何况是在 Internet 高速发展的今天。或者采取封闭与各种媒介进行数据传输的方法来解决，比如不上网、不使用光盘、软盘、移动硬盘等，可是不通过各种媒介来传输数据、工具软件，使用电脑的意义又何在？电脑的价值又怎能体现出来？因此，我们为了让电脑用户更安全的使用电脑，防止日益频繁的电脑病毒发作，以下列出 13 项防御电脑病毒的措施。

（1）使用具有自动防毒的杀毒软件（病毒防火墙）。因为只有这样才能时时刻刻保证电脑不被已知的病毒攻击。

（2）定期升级杀毒软件。因为杀毒软件的病毒库是动态的，当有新病毒出现后，病毒厂商会在第一时间内将病毒查杀代码放入病毒库，也就是说，只有及时升级病毒库才会更有效的保护电脑不被病毒攻击。

（3）使用邮件监控软件。病毒通过电子邮件进行传播，早已是众所周知的了，可是这并没有使大家提高警惕，反而对邮件的防御意识越来越轻视。笔者建议广大电脑用户在通过邮件客户端程序收取邮件时，一定要使用邮件监控软件。

（4）对来历不明的邮件即删无疑。由于邮件病毒有时会以 *.eml、*.nws、*.mht 等后缀形式的文件出现，用户在预览该文件时，这些文件携带的病毒程序会被立即执行，故

此，当有来历不明的邮件时，尽量不要打开，哪怕是贺卡之类的邮件。

（5）从网上下载的软件，在使用之前一定对其进行病毒扫描。从网上下载的软件，大部分都是压缩格式的文件，这样就使病毒有了匿身之所，当用户解压缩此文件时，病毒也就随之进行感染，再有，有些软件的安装程序已经被人进行反编辑、更改或添加，当用户下载安装后，便会出现不可预料的事情，比如 OICQ 网络寻呼机，在网上有很多可以查看好友 IP 的 OICQ，但这并不是腾讯公司推出的官方版本，所以对用户是没有任何保障的，甚至还有带木马程序的 OICQ，对于这种软件，用户千万不要只看到它具有特殊功能就进行下载，即便要下载，也要与官方版本相互对比文件大小，然后使用杀毒软件进行扫描一遍，只有这样才能在一定程度上保护电脑系统的安全。

（6）不要随便使用来历不明和未经授权的软件。因为在这些软件中，极有可能含有恶意程序代码、木马程序等，当安装使用后，就等于将自己的电脑一丝不挂的展现给互联网上的其他用户。

（7）不要去一些黑客网站、非正规网站下载软件。很多电脑用户在网上寻找软件、下载软件的过程中，大部分所关注的是下载速度，而不关注下载软件的可靠性和安全性，这就造成下载软件后，在安装、使用过程中出现安装程序文件不全、文件损坏、非法操作、程序中带有病毒等现象，既耽误了工作效率，又浪费了上网费用，最重要的是对电脑的安全缺少保障。

笔者建议，下载任何软件不仅要关注下载速率问题，更重要的是网站的知名度、安全性和版本的更新速度，因为这都影响着电脑用户的直接利益。

国内软件下载网站中，模式比较正规、知名度较高、速度快、规模大、覆盖程度广的有华军软件园、中国下载、天空软件站、Enet 软件下载、太平洋软件下载、电脑之家、海阔天空软件下载、无忧软件网等。

（8）对重要的数据要经常作备份。在电脑病毒猖狂的今天，任何事情都会发生，也许是现在、明天或后天，因此，除了做好病毒防范工作以外，应该经常对重要、机密的数据作备份或加密。

（9）在电脑系统不被病毒感染的情况下做好电脑应急启动软盘。以防止被病毒攻击时不能启动系统。

（10）使用硬盘备份工具备份硬盘数据。如果经常上网的用户更要使用象 Ghost 之类的硬盘维护工具，当被病毒攻击而又无法恢复的时候，还可以通过备份软件将系统恢复回来，以最小程度的减小损失。

（11）对于局域网用户更要做好防范病毒工作，因为目前大多数病毒都可以通过局域

网进行传染。将每台电脑所有共享文件夹都加上密码，而且还要注意，不要在输入网络密码时保存密码列表，不然，设置的密码就形同虚设了。

（12）使用光盘、软盘、移动硬盘等各种媒介时要使用杀毒软件扫描一遍，不要偷懒、省事，不要以为光盘存有病毒的几率很小，也许就在存有侥幸心理的时候，

病毒会侵入电脑系统，然后进行破坏，使系统瘫痪，相对而言，麻烦总比粗心的好，虽然每次都耽搁一些时间，但可以最大限度的保护了电脑系统的安全问题。

（13）经常观看、收听病毒新闻和报道资料，了解最新病毒动态。这样可以清楚知道病毒是怎样传染，针对什么类型的操作系统、机型，发作日期是什么时候，危害程度有多大，相对就可以做好一切防御措施，来个有备无患，不至于到时让病毒给你弄个措手不及。比如 CIH 病毒发作日期在每年的 4 月 26 日，没有重要事情的用户尽量避开这天使用电脑，如果用户在那天必须使用电脑的话，最好先在 4 月 26 日之前将电脑的系统时间向前或向后调整，使病毒不能按照常规时间发作。

1.5 杀毒软件的使用技巧

杀毒软件在使用时要讲究技巧，要结合软件的功能，比如定时查毒、自动升级、任务完成自动关闭等。笔者认为，发挥其特有的功能，会更准确、有效的查杀病毒。

（1）使用定时查毒功能，可以降低无效的等待时间（如今的硬盘容量太大了，再快的扫描引擎，等待时间也是很长的），提高工作效率，比如，设置在休息的时间段，不使用电脑的时间段进行查毒，当然，也可以设置在 4 月 26 日（CIH 病毒发作日）的前一天进行查毒工作，避免出现问题。目前，几乎所有的杀毒软件都带有定时功能。

（2）使用定时、自动升级功能，升级软件的病毒库、引擎及各种功能是预防、查杀病毒的必要手段，应该说是最重要的步骤之一了。对于具备上网条件的电脑用户，可以直接通过互联网进行升级，不过，由于大多数都是电话拨号用户，造成很多人在上网时都懒得升级，此时，可以设置自动升级功能，自动检测网站是否推出新版本的升级包，避免烦琐的手动连接。再有，由于工作等原因忘记升级也是存在的，定时自动升级功能就派上用场了，可以设置成某一时间段来进行升级，或设置成自动检测互联网连接状态，以便获得杀毒网站的升级信息。建议拨号用户每周升级一次，对于使用宽带的电脑用户，可以设置成每日一次升级。

（3）使用查杀病毒任务完成后自动关闭功能，该功能可以分成两种，一是关闭杀毒软件本身，二是关闭电脑系统，前者主要应用于有事需要离开电脑一段时间的用户，后者是应用于单位下班前、长时间离开电脑、以及晚上睡觉前想进行查毒的用户。

（4）DOS 杀毒软盘的使用

几乎所有的杀毒软件都提供一张 DOS 杀毒盘，在使用 DOS 杀毒软之前，需要制作一张 DOS 启动盘，这是因为 DOS 杀毒盘不是引导盘，不能启动电脑。在开机后，先插入 DOS 启动盘，引导进入 DOS 后，再插入 DOS 杀毒盘即可，然后通过 DOS 命令进行查杀病毒。

1.6 病毒识别、防范技巧

1.6.1 宏病毒的识别技巧

除了使用杀毒软件来检测宏病毒之外，也可以通过手动方法来查看是否感染宏病毒，虽然方法不能针对所有的宏病毒，但对于一时没有杀毒软件的用户，通过这种方法也是相当有效的。

（1）打开 Word 中的“工具”→“宏”菜单中的“宏”功能，选中 Normal.dot 模板，若发现含有 AutoOpen、AutoNew、AutoClose 等自动宏，FileSave、FileSaveAs、FileExit 等文件操作宏，以及含有 AAAZAO、PayLoad 之类的怪名称的宏，此时，很可能已经被宏病毒感染了。

（2）打开 Word 中的“工具”菜单，看不到“宏”选项，或可以看到“宏”选项，但鼠标点击“宏”功能没有反应，此时，可以肯定已经被宏病毒感染了。

（3）打开一个 Word 文档后，不对该文档进行任何操作，点击退出时，如果提示保存该文件，此时，Word 中的 Normal.dot 模板很可能已经被宏病毒感染。

（4）打开 Word 文档后，对此文档进行另存操作，却只能以模板方式进行保存，此时，很可能已经被宏病毒感染。

（5）在启动 Word 过程中出现内存不足现象，在使用过程中出现打印不正常现象，此时，很可能已经被宏病毒感染。

1.6.2 宏病毒的防范技巧

对于宏病毒是可以完全预防的，前提条件是 Office 软件未被宏病毒感染，并在使用之前进行正确的设置，具体设置方法如下：

（1）打开 Word 中的“工具”→“选项”菜单，选中“提示保存 Normal 模板”和宏病毒防护功能（一般情况是默认选项）。

（2）清理“工具”→“模板和加载项”→“共用模板及加载项”中的加载文件，当

必须加载的文件一定要确保该文件没有宏病毒，并且取消已选中的“自动更新样式”功能。

（3）当退出 Word 时，要按照提示保存 Normal.dot 模板后退出，查找 Normal.dot 文件，将该文件的属性更改成“只读”。

（4）在 Excel 和 PowerPoint 中选择“工具”→“选项”菜单，在“常规”选项中选定“宏病毒防护”功能。

（5）开启防病毒软件的防护功能，以及其它防范功能。

（6）对于打开提示有是否启用宏的文档，尽量不要启用，当然，除非你可以确保此文档中没有包含蓄意破坏的宏病毒。当退出时，除了文档以外的文件给以保存，其余的文件一律不予保存，比如 Normal.dot 模板等。

1.6.3　邮件病毒的防范技巧

对于上网的用户，电子邮件（E-Mail）这个名词并不陌生，它是上网用户经常使用的一种传送各种信息的工具，但它也是病毒传播的一种媒介，病毒可以通过它大肆传播散发，可以在极短的时间内感染上千万个用户，可以说是无孔不入。为了防止邮件病毒的入侵，除了使用病毒防火墙和邮件防火墙进行防范，还应该注意以下几点：

（1）不要轻易打开不明来历邮件中的附件，尤其是自称不可不看等具有吸引力的邮件，这类邮件很可能就是一个邮件病毒。即便发信人是比较熟悉的朋友，当邮件中带有附件时，而邮件内容中并没有提到，就不要轻易打开，如果想打开，也要仔细查看一番，因为很多病毒是通过地址薄中的邮件地址来发送带毒邮件的，它们一般都具有自动复制，查找地址薄，自动发送邮件等功能。

（2）不要设置“自动回信”功能，“自动回信”功能是方便大家在没有收信时，及时回复发信人一封确认收到回函，但如果双方用户同时开启了自动回复功能，那该功能将会给双方的邮箱带来灾难。

（3）设置邮件过滤功能，防止超过信箱容量的大邮件和邮件炸弹，当遇到此类邮件时，可以自动进行删除，以保证信箱安全。

1.6.4　特洛伊木马病毒的识别技巧

识别特洛伊木马病毒可以通过杀毒软件扫描，一般情况是可以找出的，不过避免杀毒软件没有新木马的病毒码而造成遗漏，可以通过以下两种方法：

（1）要经常观察网速的速度和收发流量，尤其是当网速突然变慢的时候，如果在数字的变化上是 1～3 Kbit/s（1～3 千字节/每秒）的话，那很有可能是特洛伊木马病毒在作

怪，再有，一般情况下，“已发送字节”应该比“接收字节”低 10 倍左右，如果“已发送字节”过多，表明有人从你的硬盘上传送数据，很可能是特洛伊木马病毒在作怪，除非你正在使用 FTP 进行上传呢。

（2）通过防火墙等软件查看与本机连接的通信进程，对于熟悉 TCP/IP 的用户也可以在 MS-DOS 方式下查看，如果出现可疑的端口与电脑相连，那可要仔细检查一下了，我们上网通常使用的端口有 80、1080 等。

（3）查看 C 盘中的非执行类文件，可以通过记事本来打开，查看在文件内有没有可疑文件纪录，再有，还要查看 C 盘 Windows 和 Windows/System 目录中的文件，如果发现只有文件名而没有图标，那可疑就是特洛伊木马病毒或其它病毒的文件了。

1.6.5 特洛伊木马病毒的防范技巧

（1）当通过以上方法查看，怀疑有特洛伊木马病毒的存在后，可以采用病毒软件对整个硬盘进行扫描，但在发现可疑现象的时候，应当立即断开与网络的连接，以便减少一些损失。

（2）在下载软件后，很多人会先看看 Readme.txt 文件，想详细了解软件的具体功能，但很多人都忽略了 Readme 文件大多是 *.txt 格式的，而不是 *.exe 格式的，希望大家在运行 Readme 文件之前要看看文件的扩展名，不要有半点疏忽，以免电脑称为特洛伊木马病毒的牺牲品。因为 Readme.exe 常常捆绑有病毒或木马程序，甚至其文件本身就是一个病毒或木马程序的服务端，只是更变了文件名称而已。

1.6.6 恢复系统技巧

当病毒已经感染了电脑系统时，第一时间就应使用杀毒软件清除，在无法清除时，且被感染的文件数量不多时，应当使用杀毒软件将染毒文件删除掉，然后使用备份文件或原始安装光盘中的文件替换被破坏的文件即可。对于感染病毒的电脑，不一定就需要格式化硬盘，格式化是意味着彻底删除所有操作系统文件、应用程序、以及各种数据等文件，所有的工作都不得不从零开始，对于少量文件受到病毒感染，使用 Format 命令来清除病毒是浪费时间，而且，如果病毒攻击了主引导记录（MBR），并修改、移动硬盘第一个扇区中的分区或主引导记录数据，此时，Format 命令将不起作用，对于 MBR 感染，可以使用 FDisk/MBR 命令来恢复 MBR 数据，当然，也可以使用杀毒软件中的修复 MBR 功能。

1.6.7　防止病毒发作的技巧

防止病毒发作除了使用病毒监控软件，还可以通过更改电脑系统的日期来躲过病毒发作，但前提条件是该病毒的激活条件是由日期来决定的，也就是说它的发作日期是在一个特定时间被激活的，以日期为激活条件的病毒有很多，以下为主流病毒的名称及发作日期：

（1）CIH 病毒的发作日期为每年的 4 月 26 日，最新变种改为每年 6 月 26 日，以及每月 26 日。

（2）TaiWan No.1（台湾一号）宏病毒的发作日期为每月 13 日。

（3）Wscript.Kak.Worm 野蛮蠕虫病毒的发作日期为每月第一天的 17 点。

（4）HappyTime 欢乐时光病毒的发作日期为“月 + 日 = 13”，5 月 8 日（第一次发作日期）。

（5）MakeLove 新型爱虫病毒的发作日期为 3、6、9、12 月的 5 日。

（6）W97M.Cerin.A 病毒的发作日期为 4 月 6 日或 8 月 31 日。

（7）黑色星期五病毒的发作日期为 13 日且是星期五。

（8）July Killer 七月杀手的发作日期为 7 月 1 日至 31 日不定。